Attorney's Docket No.: 13357-002001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Masahiro Kikuta et al. Art Unit : Unknown
Serial No. : Examiner : Unknown
Filed : July 10, 2001
Title : ELECTRONIC NOTARY METHOD AND SYSTEM

BOX PATENT APPLICATION

Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL OF PRIORITY DOCUMENT UNDER 35 USC §119

Applicant hereby confirms his claim of priority under 35 USC §119 from Japan Application No. 2000-208913 filed July 10, 2000. A certified copy of the application from which priority is claimed is submitted herewith.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 7-10-01

Y. Rocky Tsao
Reg. No. 34,053

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

20286323.doc

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EL445371081US

I hereby certify under 37 CFR §1.10 that this correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, Washington, D.C. 20231.

July 10, 2001
Date of Deposit

Samantha Bell
Signature

Samantha Bell
Typed or Printed Name of Person Signing Certificate

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年 ７月１０日

出願番号
Application Number: 特願２０００－２０８９１３

出願人
Applicant (s): 亜細亜証券印刷株式会社
株式会社シナジー・インキュベート

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１０月２０日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０８７４０１

【書類名】　特許願
【整理番号】　A000002778
【提出日】　平成12年 7月10日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　1/00
【発明の名称】　電子公証システムおよび電子公証方法
【請求項の数】　16
【発明者】
　【住所又は居所】　東京都渋谷区富ケ谷一丁目３０番２２号　株式会社シナジー・インキュベート内
　【氏名】　菊田　昌弘
【発明者】
　【住所又は居所】　東京都渋谷区富ケ谷一丁目３０番２２号　株式会社シナジー・インキュベート内
　【氏名】　渡邊　修
【特許出願人】
　【住所又は居所】　東京都港区虎ノ門１丁目２５番７号
　【氏名又は名称】　亜細亜証券印刷株式会社
【特許出願人】
　【住所又は居所】　東京都渋谷区富ケ谷一丁目３０番２２号
　【氏名又は名称】　株式会社　シナジー・インキュベート
【代理人】
　【識別番号】　100058479
　【弁理士】
　【氏名又は名称】　鈴江　武彦
　【電話番号】　03-3502-3181
【選任した代理人】
　【識別番号】　100084618
　【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子公証システムおよび電子公証方法

【特許請求の範囲】

【請求項１】　公証サーバと、この公証サーバとネットワーク通信が可能な第１の端末装置および第２の端末装置とからなる電子公証システムにおいて、

前記第１の端末装置は、

ユーザが指定する電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、

前記ユーザを識別する第１のユーザ識別情報を入力する入力手段と、

前記公証サーバより予め与えられた第２のユーザ識別情報を用いて、前記公証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記メッセージデータと、前記入力手段より入力された第１のユーザ識別情報を前記公証サーバに送信し、登録鍵を受信する第１の端末側通信手段とを備え、

前記公証サーバは、

前記ユーザの第１のユーザ識別情報と、前記ユーザに予め与えた第２のユーザ識別情報を対応づけて記憶する第１の記憶手段と、

前記第１の端末側通信手段より送られる第２のユーザ識別情報と、前記第１の記憶手段に記憶される第２のユーザ識別情報が一致する場合に、前記第１の端末側通信手段との間に通信リンクを開設し通信する第１の通信手段と、

この第１の通信手段を通じて前記第１の端末装置よりメッセージデータを受信すると、登録鍵を生成し、前記第１の通信手段を通じて前記第１の端末装置に送信する登録鍵生成手段と、

前記第１の通信手段を通じて受信した第１のユーザ識別情報と、前記第１の記憶手段に記憶される第１のユーザ識別情報が一致する場合に、前記第１の通信手段を通じて受信したメッセージデータを、少なくとも前記登録鍵と日時情報に対応づけて記憶する第２の記憶手段とを備え、

前記第２の端末装置は、

電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、

前記公証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記メッセージデータと登録鍵を前記公証サーバに送信する第２の端末側通信手段を備え、

前記公証サーバは、

前記第２の端末側通信手段との間に通信リンクを開設し通信する第２の通信手段と、

この第２の通信手段を通じて受信した前記メッセージデータと、前記第２の記憶手段に記憶され、前記第２の通信手段を通じて受信した登録鍵に対応するメッセージデータが一致する場合に、この一致を証明する公証情報を生成し、前記第２の通信手段を通じて前記第２の端末装置に送信する公証情報生成手段とを具備することを特徴とする電子公証システム。

【請求項２】　前記第１の端末装置は、

ユーザが指定する電子ファイルと、この電子ファイルに基づいて生成されたメッセージデータと、前記電子ファイルに対応する登録鍵を一体化した謄本情報を生成し、前記第１の端末側通信手段を通じて前記公証サーバに送信する謄本生成手段を備え、

前記公証サーバは、

前記第１の通信手段を通じて受信した前記謄本情報に含まれる情報に対応づけて、請求鍵を生成する請求鍵生成手段と、

前記第１の通信手段を通じて受信した前記謄本情報に含まれるメッセージデータと、前記第２の記憶手段に記憶され、前記謄本情報に含まれる登録鍵に対応するメッセージデータとが一致し、なおかつ前記第１の通信手段を通じて受信した第１のユーザ識別情報と、前記第１の記憶手段に記憶される第１のユーザ識別情報が一致する場合に、前記謄本情報に含まれる電子ファイルを前記請求鍵に対応づけて謄本ファイルとして記憶する第３の記憶手段を備え、

前記第２の端末装置は、

請求鍵を含む謄本要求情報を生成し、この謄本要求情報を前記第２の端末側通信手段を通じて前記公証サーバに送信する謄本要求手段を備え、

前記公証サーバは、

前記第２の通信手段を通じて受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、前記第３の記憶手段より読み出して、前記第２の通信手段を通じて前記第２の端末装置に送信する謄本ファイル送信制御手段とを備えることを特徴とする請求項１に記載の電子公証システム。

【請求項３】　公証サーバと、この公証サーバとネットワーク通信が可能な第１の端末装置および第２の端末装置とからなる電子公証システムにおいて、

前記第１の端末装置は、

前記ユーザを識別する第１のユーザ識別情報を入力する入力手段と、

ユーザが指定する電子ファイルを含む謄本情報を生成する謄本生成手段と、

前記公証サーバより予め与えられた第２のユーザ識別情報を用いて、前記公証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記謄本情報と、前記入力手段より入力された第１のユーザ識別情報を前記公証サーバに送信する第１の端末側通信手段とを備え、

前記公証サーバは、

前記ユーザの第１のユーザ識別情報と、前記ユーザに予め与えた第２のユーザ識別情報を対応づけて記憶する第１の記憶手段と、

前記第１の端末側通信手段より送られる第２のユーザ識別情報と、前記第１の記憶手段に記憶される第２のユーザ識別情報が一致する場合に、前記第１の端末側通信手段との間に通信リンクを開設し通信する第１の通信手段と、

この第１の通信手段を通じて受信した前記謄本情報に含まれる電子ファイルに対応づけて、請求鍵を生成する請求鍵生成手段と、

前記第１の通信手段を通じて受信した第１のユーザ識別情報と、前記第１の記憶手段に記憶される第１のユーザ識別情報が一致する場合に、前記謄本情報に含まれる電子ファイルを、少なくとも前記請求鍵と日時情報に対応づけて謄本ファイルとして記憶する第３の記憶手段を備え、

前記第２の端末装置は、

前記公証サーバとの間に通信リンクを開設して通信する第２の端末側通信手段と、

請求鍵を含む謄本要求情報を生成し、この謄本要求情報を前記第２の端末側

通信手段を通じて前記公証サーバに送信する謄本要求手段を備え、

前記公証サーバは、

前記第２の端末側通信手段との間に通信リンクを開設し通信する第２の通信手段と、

この第２の通信手段を通じて受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、前記第３の記憶手段より読み出して、前記第２の通信手段を通じて前記第２の端末装置に送信する謄本ファイル送信制御手段とを備えることを特徴とする電子公証システム。

【請求項４】　前記ネットワーク上に、前記請求鍵を取得可能なＷｅｂを有するＷｅｂサーバを備え、

前記公証サーバは、

前記第１の端末装置より指定される電子メールアドレス宛てに、前記ＷｅｂのＵＲＬ情報を電子メールにて送信するＵＲＬ情報通知手段を備えることを特徴とする請求項２または請求項３に記載の電子公証システム。

【請求項５】　前記謄本ファイル送信制御手段が電子ファイルを前記第２の端末装置に送信した場合に、前記第２の端末装置から謄本要求情報を受信した時刻と、前記電子ファイルを前記第２の端末装置に送信した時刻のうち、少なくとも一方を記憶する第４の記憶手段を備えることを特徴とする請求項２または請求項３に記載の電子公証システム。

【請求項６】　前記第１のユーザ識別情報は、前記ユーザのバイオメトリック情報であることを特徴とする請求項１乃至請求項５のいずれかに記載の電子公証システム。

【請求項７】　公証サーバと、この公証サーバとネットワーク通信が可能な端末装置とからなる電子公証システムにおいて、

前記端末装置は、

ユーザが指定する電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、

前記ユーザを識別する第１のユーザ識別情報を入力する入力手段と、

前記公証サーバより予め与えられた第２のユーザ識別情報を用いて、前記公

証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記メッセージデータと、前記入力手段より入力された第１のユーザ識別情報を前記公証サーバに送信し、登録鍵を受信する端末側通信手段とを備え、

前記公証サーバは、

前記ユーザの第１のユーザ識別情報と、前記ユーザに予め与えた第２のユーザ識別情報を対応づけて記憶する第１の記憶手段と、

前記端末側通信手段より送られる第２のユーザ識別情報と、前記第１の記憶手段に記憶される第２のユーザ識別情報が一致する場合に、前記端末側通信手段との間に通信リンクを開設し通信する通信手段と、

この通信手段を通じて前記端末装置よりメッセージデータを受信すると、登録鍵を生成し、前記通信手段を通じて前記端末装置に送信する登録鍵生成手段と、

前記通信手段を通じて受信した第１のユーザ識別情報と、前記第１の記憶手段に記憶される第１のユーザ識別情報が一致する場合に、前記通信手段を通じて受信したメッセージデータを、少なくとも前記登録鍵と日時情報に対応づけて記憶する第２の記憶手段とを具備することを特徴とする電子公証システム。

【請求項８】　公証サーバと、この公証サーバとネットワーク通信が可能な端末装置とからなる電子公証システムにおいて、

前記端末装置は、

電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、

前記公証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記メッセージデータと登録鍵を前記公証サーバに送信する端末側通信手段を備え、

前記公証サーバは、

電子ファイルのメッセージデータを、少なくとも登録鍵と日時情報に対応づけて記憶する記憶手段と、

前記端末側通信手段との間に通信リンクを開設し通信する通信手段と、

この通信手段を通じて受信した前記メッセージデータと、前記記憶手段に記

憶され、前記通信手段を通じて受信した登録鍵に対応するメッセージデータが一致する場合に、この一致を証明する公証情報を生成し、前記通信手段を通じて前記端末装置に送信する公証情報生成手段とを具備することを特徴とする電子公証システム。

【請求項９】　公証サーバと、この公証サーバとネットワーク通信が可能な端末装置とからなる電子公証システムにおいて、

前記端末装置は、

前記ユーザを識別する第１のユーザ識別情報を入力する入力手段と、

ユーザが指定する電子ファイルを含む謄本情報を生成する謄本生成手段と、

前記公証サーバより予め与えられた第２のユーザ識別情報を用いて、前記公証サーバとの間に通信リンクを開設して通信するもので、少なくとも前記謄本情報と、前記入力手段より入力された第１のユーザ識別情報を前記公証サーバに送信する端末側通信手段とを備え、

前記公証サーバは、

前記ユーザの第１のユーザ識別情報と、前記ユーザに予め与えた第２のユーザ識別情報を対応づけて記憶する第１の記憶手段と、

前記端末側通信手段より送られる第２のユーザ識別情報と、前記第１の記憶手段に記憶される第２のユーザ識別情報が一致する場合に、前記端末側通信手段との間に通信リンクを開設し通信する通信手段と、

この通信手段を通じて受信した前記謄本情報に含まれる電子ファイルに対応づけて、請求鍵を生成する請求鍵生成手段と、

前記通信手段を通じて受信した第１のユーザ識別情報と、前記第１の記憶手段に記憶される第１のユーザ識別情報が一致する場合に、前記謄本情報に含まれる電子ファイルを、少なくとも前記請求鍵と日時情報に対応づけて謄本ファイルとして記憶する第２の記憶手段とを具備することを特徴とする電子公証システム。

【請求項１０】　公証サーバと、この公証サーバとネットワーク通信が可能な端末装置とからなる電子公証システムにおいて、

前記端末装置は、

前記公証サーバとの間に通信リンクを開設して通信する端末側通信手段と、

請求鍵を含む謄本要求情報を生成し、この謄本要求情報を前記端末側通信手段を通じて前記公証サーバに送信する謄本要求手段を備え、

前記公証サーバは、

電子ファイルを、少なくとも請求鍵と日時情報に対応づけて謄本ファイルとして記憶する記憶手段を備え、

前記端末側通信手段との間に通信リンクを開設し通信する通信手段と、

この通信手段を通じて受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、前記記憶手段より読み出して、前記通信手段を通じて前記端末装置に送信する謄本ファイル送信制御手段とを具備することを特徴とする電子公証システム。

【請求項１１】　公証サーバと、この公証サーバとネットワーク通信が可能な第１の端末装置および第２の端末装置とからなる電子公証システムで用いられる電子公証方法において、

前記公証サーバが、前記第１の端末装置のユーザの第１のユーザ識別情報と、前記ユーザに予め与えた第２のユーザ識別情報を対応づけて記憶する第１の記憶工程と、

前記第１の端末装置が、前記ユーザが指定する電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成工程と、

前記第１の端末装置が、前記ユーザを識別する第１のユーザ識別情報を受け付ける受付工程と、

前記第１の端末装置が、前記公証サーバより予め与えられた第２のユーザ識別情報を前記公証サーバに送信し、この第２のユーザ識別情報が前記公証サーバにおいて、前記第１の記憶工程にて記憶された第２のユーザ識別情報と一致する場合に、前記第１の端末装置と前記公証サーバの間に前記第１の通信リンクを開設する第１の通信リンク開設工程と、

前記第１の端末装置が前記公証サーバに対して、前記第１の通信リンクを通じて、少なくとも前記固有メッセージ生成工程にて生成したメッセージデータと、前記受付工程にて受け付けた第１のユーザ識別情報を送信する公証登録要求工程

と、

前記公証サーバが、前記第１の通信リンクを通じて前記第１の端末装置よりメッセージデータを受信すると、登録鍵を生成し、前記第１の通信リンクを通じて前記第１の端末装置に送信する登録鍵生成工程と、

前記公証サーバが、前記第１の通信リンクを通じて受信した前記第１のユーザ識別情報と、前記第１の記憶工程で記憶される第１のユーザ識別情報が一致する場合に、前記第１の通信リンクを通じて受信したメッセージデータを、少なくとも前記登録鍵と日時情報に対応づけて記憶する第２の記憶工程と、

前記第２の端末装置が、電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成工程と、

前記第２の端末装置と前記公証サーバとの間に第２の通信リンクを開設して通信する第２の通信リンク開設工程と、

前記第２の端末装置が、前記第２の通信リンクを通じて、少なくとも前記メッセージデータと登録鍵を前記公証サーバに送信する公証要求工程と、

前記公証サーバが、前記第２の通信リンクを通じて受信した前記メッセージデータと、前記第２の記憶工程にて記憶され前記第２の通信リンクを通じて受信した登録鍵に対応するメッセージデータが一致する場合に、この一致を証明する公証情報を生成し、前記第２の通信リンクを通じて前記第２の端末装置に送信する公証情報生成工程とを具備することを特徴とする電子公証方法。

【請求項１２】　前記第１の端末装置が、ユーザが指定する電子ファイルと、この電子ファイルに基づいて生成されたメッセージデータと、前記電子ファイルに対応する登録鍵を一体化した謄本情報を生成し、前記第１の通信リンクを通じて前記公証サーバに送信する謄本生成工程と、

前記公証サーバが、前記第１の通信リンクを通じて受信した前記謄本情報に含まれる情報に対応づけて、請求鍵を生成する請求鍵生成工程と、

前記公証サーバが、前記第１の通信リンクを通じて受信した前記謄本情報に含まれるメッセージデータと、前記第２の記憶工程にて記憶され前記謄本情報に含まれる登録鍵に対応するメッセージデータとが一致し、なおかつ前記第１の通信リンクを通じて受信した第１のユーザ識別情報と、前記第１の記憶工程にて記憶

される第１のユーザ識別情報が一致する場合に、前記謄本情報に含まれる電子ファイルを前記請求鍵に対応づけて謄本ファイルとして記憶する第３の記憶工程と、

前記第２の端末装置が、請求鍵を含む謄本要求情報を生成し、この謄本要求情報を前記公証サーバに送信する謄本要求工程と、

前記公証サーバが、前記第２の端末装置より受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、前記第３の記憶工程で記憶した情報より読み出して、前記第２の端末装置に送信する謄本ファイル送信工程とを備えることを特徴とする請求項１１に記載の電子公証方法。

【請求項１３】　公証サーバと、この公証サーバとネットワーク通信が可能な第１の端末装置および第２の端末装置とからなる電子公証システムで用いられる電子公証方法において、

前記公証サーバが、前記第１の端末装置のユーザの第１のユーザ識別情報と、前記ユーザに予め与えた第２のユーザ識別情報を対応づけて記憶する第１の記憶工程と、

前記第１の端末装置が、前記ユーザを識別する第１のユーザ識別情報を受け付ける受付工程と、

前記第１の端末装置が、ユーザが指定する電子ファイルを含む謄本情報を生成する謄本生成工程と、

前記第１の端末装置が、前記公証サーバより予め与えられた第２のユーザ識別情報を前記公証サーバに送信し、この第２のユーザ識別情報が前記公証サーバにおいて、前記第１の記憶工程にて記憶された第２のユーザ識別情報と一致する場合に、前記第１の端末装置と前記公証サーバの間に前記第１の通信リンクを開設する第１の通信リンク開設工程と、

前記第１の端末装置が前記公証サーバに対して、前記第１の通信リンクを通じて、少なくとも前記謄本生成工程にて生成した謄本情報と、前記受付工程にて受け付けた第１のユーザ識別情報を送信する謄本登録要求工程と、

前記公証サーバが、前記第１の通信リンクを通じて前記第１の端末装置より謄本情報を受信すると、請求鍵を生成する請求鍵生成工程と、

前記公証サーバが、前記第１の通信リンクを通じて受信した第１のユーザ識別情報と、前記第１の記憶工程で記憶される第１のユーザ識別情報が一致する場合に、前記謄本情報に含まれる電子ファイルを、少なくとも前記請求鍵と日時情報に対応づけて謄本ファイルとして記憶する第３の記憶工程と、

前記第２の端末装置と前記公証サーバとの間に第２の通信リンクを開設して通信する第２の通信リンク開設工程と、

前記第２の端末装置が、前記第２の通信リンクを通じて、請求鍵を含む謄本要求情報を生成し、この謄本要求情報を前記公証サーバに送信する謄本要求工程と、

前記公証サーバが、前記第２の通信リンクを通じて受信した前記謄本要求情報に含まれる請求鍵に対応する電子ファイルを、前記第３の記憶工程にて記憶した情報より読み出して、前記第２の通信リンクを通じて前記第２の端末装置に送信する謄本ファイル送信工程とを備えることを特徴とする電子公証方法。

【請求項１４】　前記ネットワーク上に、前記請求鍵を取得可能なＷｅｂを有するＷｅｂサーバを備え、

前記公証サーバにおいて、前記第１の端末装置より指定される電子メールアドレス宛てに、前記ＷｅｂのＵＲＬ情報を電子メールにて送信するＵＲＬ情報通知工程を備えることを特徴とする請求項１２または請求項１３に記載の電子公証方法。

【請求項１５】　前記謄本ファイル送信工程が電子ファイルを前記第２の端末装置に送信した場合に、前記第２の端末装置から謄本要求情報を受信した時刻と、前記電子ファイルを前記第２の端末装置に送信した時刻のうち、少なくとも一方を記憶する第４の記憶工程を備えることを特徴とする請求項１２または請求項１３に記載の電子公証方法。

【請求項１６】　前記第１のユーザ識別情報は、前記ユーザのバイオメトリック情報であることを特徴とする請求項１１乃至請求項１５のいずれかに記載の電子公証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、例えばインターネットなどのコンピュータネットワークを通じて、電子化された文書の公証を行う電子公証システムに関する。

【０００２】

【従来の技術】

周知のように、近時、インターネットなどのコンピュータネットワークを通じて契約や商取引などが行われるようになり、今後、このようなネットワーク利用は、さらに発展すると見込まれている。このようなネットワーク利用を支える認証技術の１つとして、電子署名がある。

【０００３】

この電子署名は、ネットワーク上でやりとりされるデジタル情報に署名情報を付加して、デジタル情報の正当性を保証する技術で、署名には公開鍵暗号が用いられる。この公開鍵は、認証局（ＣＡ：Certificate Authority）といわれる第三者機関により、その正当性が保証される。

【０００４】

以下、図７を参照して、その一例を説明する。

【０００５】

署名者（送信者）は、送信する文書Ｍからハッシュ関数ｈを用いて特徴値を生成し、これと自分だけが知っている秘密鍵から署名文Ｄ（ｈ（Ｍ））を作る。そして、署名文Ｄ（ｈ（Ｍ））と元の文書Ｍを一緒に相手に送る。

【０００６】

これに対して、検証者（受信者）は、受け取った署名文Ｄ（ｈ（Ｍ））を署名者の公開鍵で解き、上記ｈ（Ｍ）を得る。また、受信した元の文書Ｍをハッシュ関数ｈで圧縮し、この圧縮結果ｈ（Ｍ）と、上述のように公開鍵で解いたｈ（Ｍ）を比較して、署名が正しいかどうかを検査することにより、受信した文書Ｍの正当性を確認する。

【０００７】

この他に、文書の送信者を識別する方法として、虹彩認証や声紋認証、サイン鑑定などの認証技術も開発されている。

以上のような認証技術を用いて、電子化された文書に電子署名して保証を行うことにより、悪意のある第三者が正当な署名者になりすまして、文書を偽造することが防止できる。

【０００８】

しかしながら、例えば同一の取引に関して正当な署名者が、複数の異なる内容の文書に電子署名を行った場合、どの文書が正しい文書であるか確認する必要が生じる。

【０００９】

さらに、このように複数の異なる内容の署名文書が存在する場合に、例えば遺言状のように署名者本人によって確認が行えないものの際には、どの文書が正当なものであるかを確認できないという問題が生じる。

【００１０】

【発明が解決しようとする課題】

従来の技術では、ネットワーク上でやりとりされる文書を公証するには不十分であるという問題があった。

この発明は上記の問題を解決すべくなされたもので、ネットワーク上でやりとりされる文書に対して、信頼性の高い公証を行うことが可能な電子公証システムおよび電子公証方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】

上記の目的を達成するために、請求項１に係わる本発明は、公証サーバと、この公証サーバとネットワーク通信が可能な第１の端末装置および第２の端末装置とからなる電子公証システムにおいて、第１の端末装置は、ユーザが指定する電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、ユーザを識別する第１のユーザ識別情報を入力する入力手段と、公証サーバより予め与えられた第２のユーザ識別情報を用いて、公証サーバとの間に通信リンクを開設して通信するもので、少なくともメッセージデータと、入力手段より入力された第１のユーザ識別情報を公証サーバに送信し、登録鍵を受信する第１の端末側通信手段とを備え、公証サーバは、ユーザの第１のユー

ザ識別情報と、ユーザに予め与えた第２のユーザ識別情報を対応づけて記憶する第１の記憶手段と、第１の端末側通信手段より送られる第２のユーザ識別情報と、第１の記憶手段に記憶される第２のユーザ識別情報が一致する場合に、第１の端末側通信手段との間に通信リンクを開設し通信する第１の通信手段と、この第１の通信手段を通じて第１の端末装置よりメッセージデータを受信すると、登録鍵を生成し、第１の通信手段を通じて第１の端末装置に送信する登録鍵生成手段と、第１の通信手段を通じて受信した第１のユーザ識別情報と、第１の記憶手段に記憶される第１のユーザ識別情報が一致する場合に、第１の通信手段を通じて受信したメッセージデータを、少なくとも登録鍵と日時情報に対応づけて記憶する第２の記憶手段とを備え、第２の端末装置は、電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成手段と、公証サーバとの間に通信リンクを開設して通信するもので、少なくともメッセージデータと登録鍵を公証サーバに送信する第２の端末側通信手段を備え、公証サーバは、第２の端末側通信手段との間に通信リンクを開設し通信する第２の通信手段と、この第２の通信手段を通じて受信したメッセージデータと、第２の記憶手段に記憶され、第２の通信手段を通じて受信した登録鍵に対応するメッセージデータが一致する場合に、この一致を証明する公証情報を生成し、第２の通信手段を通じて第２の端末装置に送信する公証情報生成手段とを具備して構成するようにした。

【００１２】

また、請求項１１に係わる本発明は、公証サーバと、この公証サーバとネットワーク通信が可能な第１の端末装置および第２の端末装置とからなる電子公証システムで用いられる電子公証方法において、公証サーバが、第１の端末装置のユーザの第１のユーザ識別情報と、ユーザに予め与えた第２のユーザ識別情報を対応づけて記憶する第１の記憶工程と、第１の端末装置が、ユーザが指定する電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成工程と、第１の端末装置が、ユーザを識別する第１のユーザ識別情報を受け付ける受付工程と、第１の端末装置が、公証サーバより予め与えられた第２のユーザ識別情報を公証サーバに送信し、この第２のユーザ識別情報が公証サー

バにおいて、第１の記憶工程にて記憶された第２のユーザ識別情報と一致する場合に、第１の端末装置と公証サーバの間に第１の通信リンクを開設する第１の通信リンク開設工程と、第１の端末装置が公証サーバに対して、第１の通信リンクを通じて、少なくとも固有メッセージ生成工程にて生成したメッセージデータと、受付工程にて受け付けた第１のユーザ識別情報を送信する公証登録要求工程と、公証サーバが、第１の通信リンクを通じて第１の端末装置よりメッセージデータを受信すると、登録鍵を生成し、第１の通信リンクを通じて第１の端末装置に送信する登録鍵生成工程と、公証サーバが、第１の通信リンクを通じて受信した第１のユーザ識別情報と、第１の記憶工程で記憶される第１のユーザ識別情報が一致する場合に、第１の通信リンクを通じて受信したメッセージデータを、少なくとも登録鍵と日時情報に対応づけて記憶する第２の記憶工程と、第２の端末装置が、電子ファイルから、この電子ファイル固有のメッセージデータを生成する固有メッセージ生成工程と、第２の端末装置と公証サーバとの間に第２の通信リンクを開設して通信する第２の通信リンク開設工程と、第２の端末装置が、第２の通信リンクを通じて、少なくとも前記メッセージデータと登録鍵を公証サーバに送信する公証要求工程と、公証サーバが、第２の通信リンクを通じて受信したメッセージデータと、第２の記憶工程にて記憶され第２の通信リンクを通じて受信した登録鍵に対応するメッセージデータが一致する場合に、この一致を証明する公証情報を生成し、第２の通信リンクを通じて第２の端末装置に送信する公証情報生成工程とを具備して構成するようにした。

【００１３】

上記構成の電子公証システムおよび電子公証方法では、電子ファイルの公証登録を行なう場合には、第１の端末装置にて、予め与えられたユーザ識別情報を用いて公証サーバとの間に通信リンクを開設し、公証対象となる電子ファイルの固有のメッセージデータを作成して公証サーバに送信する。

【００１４】

これに対して公証サーバは、第１の端末装置よりメッセージデータを受信すると、登録鍵を作成し、第１の端末装置から送られるバイオメトリック情報などの第１のユーザ識別情報に基づいて、第１の端末装置のユーザが正当な者であるこ

とを識別すると、上記登録鍵を上記電子ファイルに対応づけて記憶する。

【００１５】

一方、手元の電子ファイルが公証されたものであるか確認する場合には、第２の端末装置により、上記電子ファイルの固有のメッセージデータを作成し、このメッセージデータと、電子ファイルとともに入手した登録鍵を公証サーバに送信する。

【００１６】

これに対して、公証サーバは、受信した登録鍵に対応するメッセージデータを読み出し、このメッセージデータと、第２の端末装置より受信したメッセージデータが一致する場合には、その旨を示す公証情報を作成し、第２の端末装置に送信するようにしている。

【００１７】

したがって、上記構成の電子公証システムおよび電子公証方法によれば、悪意を有する第三者が、第１の端末装置のユーザになりすまして電子ファイルを公証登録しようとしても、上記ユーザの識別情報や、バイオメトリック情報などの第１のユーザ識別情報の入力が必要なため、なりすましによる不正公証登録を確実に防止できる。

【００１８】

すなわち、上記構成の電子公証システムおよび電子公証方法によれば、公証サーバにより公証される電子ファイルは、公証人役場で公証される紙媒体の公正証書と同様に、真正性が保証された公証が行われたものであり、公証確認を求める者はネットワークを通じて迅速かつ正確な公証サービスを受けることができる。

【００１９】

そしてまた、請求項３に係わる本発明は、公証サーバと、この公証サーバとネットワーク通信が可能な第１の端末装置および第２の端末装置とからなる電子公証システムにおいて、第１の端末装置は、ユーザを識別する第１のユーザ識別情報を入力する入力手段と、ユーザが指定する電子ファイルを含む謄本情報を生成する謄本生成手段と、公証サーバより予め与えられた第２のユーザ識別情報を用いて、公証サーバとの間に通信リンクを開設して通信するもので、少なくとも謄

本情報と、入力手段より入力された第１のユーザ識別情報を公証サーバに送信する第１の端末側通信手段とを備え、公証サーバは、ユーザの第１のユーザ識別情報と、ユーザに予め与えた第２のユーザ識別情報を対応づけて記憶する第１の記憶手段と、第１の端末側通信手段より送られる第２のユーザ識別情報と、第１の記憶手段に記憶される第２のユーザ識別情報が一致する場合に、第１の端末側通信手段との間に通信リンクを開設し通信する第１の通信手段と、この第１の通信手段を通じて受信した謄本情報に含まれる電子ファイルに対応づけて、請求鍵を生成する請求鍵生成手段と、第１の通信手段を通じて受信した第１のユーザ識別情報と、第１の記憶手段に記憶される第１のユーザ識別情報が一致する場合に、謄本情報に含まれる電子ファイルを、少なくとも請求鍵と日時情報に対応づけて謄本ファイルとして記憶する第３の記憶手段を備え、第２の端末装置は、公証サーバとの間に通信リンクを開設して通信する第２の端末側通信手段と、請求鍵を含む謄本要求情報を生成し、この謄本要求情報を第２の端末側通信手段を通じて公証サーバに送信する謄本要求手段を備え、公証サーバは、第２の端末側通信手段との間に通信リンクを開設し通信する第２の通信手段と、この第２の通信手段を通じて受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、第３の記憶手段より読み出して、第２の通信手段を通じて第２の端末装置に送信する謄本ファイル送信制御手段を具備して構成するようにした。

【００２０】

さらにまた、請求項１３に係わる本発明は、公証サーバと、この公証サーバとネットワーク通信が可能な第１の端末装置および第２の端末装置とからなる電子公証システムで用いられる電子公証方法において、公証サーバが、第１の端末装置のユーザの第１のユーザ識別情報と、ユーザに予め与えた第２のユーザ識別情報を対応づけて記憶する第１の記憶工程と、第１の端末装置が、ユーザを識別する第１のユーザ識別情報を受け付ける受付工程と、第１の端末装置が、ユーザが指定する電子ファイルを含む謄本情報を生成する謄本生成工程と、第１の端末装置が、公証サーバより予め与えられた第２のユーザ識別情報を公証サーバに送信し、この第２のユーザ識別情報が前記公証サーバにおいて、第１の記憶工程にて記憶された第２のユーザ識別情報と一致する場合に、第１の端末装置と公証サー

バの間に第１の通信リンクを開設する第１の通信リンク開設工程と、第１の端末装置が公証サーバに対して、第１の通信リンクを通じて、少なくとも謄本生成工程にて生成した謄本情報と、受付工程にて受け付けた第１のユーザ識別情報を送信する謄本登録要求工程と、公証サーバが、第１の通信リンクを通じて第１の端末装置より謄本情報を受信すると、請求鍵を生成する請求鍵生成工程と、公証サーバが、第１の通信リンクを通じて受信した第１のユーザ識別情報と、第１の記憶工程で記憶される第１のユーザ識別情報が一致する場合に、謄本情報に含まれる電子ファイルを、少なくとも請求鍵と日時情報に対応づけて謄本ファイルとして記憶する第３の記憶工程と、第２の端末装置と前証サーバとの間に第２の通信リンクを開設して通信する第２の通信リンク開設工程と、第２の端末装置が、第２の通信リンクを通じて、請求鍵を含む謄本要求情報を生成し、この謄本要求情報を公証サーバに送信する謄本要求工程と、公証サーバが、第２の通信リンクを通じて受信した謄本要求情報に含まれる請求鍵に対応する電子ファイルを、第３の記憶工程にて記憶した情報より読み出して、第２の通信リンクを通じて第２の端末装置に送信する謄本ファイル送信工程とを具備して構成するようにした。

【００２１】

上記構成の電子公証システムおよび電子公証方法では、電子ファイルの謄本登録を行なう場合には、第１の端末装置にて、予め与えられたユーザ識別情報を用いて公証サーバとの間に通信リンクを開設し、謄本となる電子ファイルを公証サーバに送信する。

【００２２】

これに対して公証サーバは、第１の端末装置より電子ファイルを受信すると、請求鍵を作成し、第１の端末装置から送られるバイオメトリック情報などの第１のユーザ識別情報に基づいて、第１の端末装置のユーザが正当な者であることを識別すると、上記請求鍵を上記電子ファイルに対応づけて記憶する。

【００２３】

一方、謄本登録された電子ファイルを取得する場合には、第２の端末装置より請求鍵を公証サーバに送信する。

これに対して、公証サーバは、受信した請求鍵に対応する電子ファイルを読み

出し、第２の端末装置に送信するようにしている。

【００２４】

したがって、上記構成の電子公証システムおよび電子公証方法によれば、悪意を有する第三者が、第１の端末装置のユーザになりすまして電子ファイルを謄本登録しようとしても、上記ユーザの識別情報や、バイオメトリック情報などの第１のユーザ識別情報の入力が必要なため、なりすましによる不正謄本登録を確実に防止できる。

【００２５】

すなわち、上記構成の電子公証システムおよび電子公証方法によれば、公証サーバに謄本登録された電子ファイルは、公証人役場で謄本登録される紙媒体の公正証書と同様に、真正性が保証された公証が行われたものであり、謄本の写しを求める者はネットワークを通じて迅速かつ正確な公証サービスを受けることができる。

【００２６】

【発明の実施の形態】

以下、図面を参照して、この発明の一実施形態について説明する。

図１は、この発明の一実施形態に係わる電子公証システムの構成を示すものである。

【００２７】

電子公証システムは、会員利用者端末１００と、公証サーバ２００と、一般利用者端末３００とをからなり、これらは、インターネットなどのコンピュータネットワークを通じて接続される。

【００２８】

会員利用者端末１００は、公証サービスに加入した会員利用者が使用するパーソナルコンピュータであって、ネットワーク通信を実現するためのハードウェアと、ネットワーク上のメールサーバと電子メールを送受信するための電子メールソフトウェアや、ネットワーク上のＷｅｂサーバに蓄積されるデータを閲覧するブラウザソフトウェアを備える。この他、会員利用者端末１００には、上記公証サービスを受けるための専用のクライアントソフトウェアがハードディスクなど

の記録媒体に組み込んである。

【００２９】

また、会員利用者端末１００は、ネットワーク上で自己を証明するためのデジタル証明書を予め取得している。このデジタル証明書は、基本フォーマットが例えばＩＴＵ－Ｔ（Telecommunication Standardization Sector）のＸ．５０９に準拠するもので、認証サービスを提供する第三者機関にて発行されたものである。

【００３０】

さらに、会員利用者端末１００は、パッド１０１を備える。パッド１０１は、サイン入力を行うための入力デバイスで、平板上に専用ペンで描かれたサインを電子データに変換する。そして、会員利用者端末１００が、上記電子データに基づいて、上記サインの筆圧や速度をサイン情報として求める。

【００３１】

公証サーバ２００は、当該公証サービスの中枢をなすサーバマシンであり、メールサーバ、Ｗｅｂサーバとしての機能を備える他、各会員のアカウント情報に対応づけて、デジタル証明書、サイン情報、電子メールアドレス、公証登録したファイルやそれに関連する種々の情報を記録可能なデータベース２０１を備える。

また、公証サーバ２００は、ネットワークやＧＰＳ衛星、あるいは電波時計などより、高精度な時刻情報を取得する機能を持つ。

【００３２】

一般利用者端末３００は、当該公証サービスにて公証された電子ファイルを取得した、あるいは取得した一般利用者が使用するパーソナルコンピュータであり、ネットワーク通信を実現するためのハードウェアと、ネットワーク上のメールサーバと電子メールを送受信するための電子メールソフトウェアや、ネットワーク上のＷｅｂサーバに蓄積されるデータを閲覧するブラウザソフトウェアを備える。

【００３３】

この他、一般利用者端末３００は、公証要求や謄本請求を行うためのクライア

ントソフトウェアを、予め上記公証サービスより取得し、ハードディスクなどの記録媒体に組み込んでいる。

なお、一般利用者端末３００は、上記クライアントソフトウェアが組み込まれた会員利用者端末１００でも代用可能である。

【００３４】

次に、上記構成の電子公証システムの動作について説明する。

まず、当該公証サービスに会員登録済み（アカウント取得済み）の会員利用者が会員利用者端末１００を通じて、任意の電子ファイルの公証情報を公証サーバ２００に登録する際の動作について説明する。図２は、この際の会員利用者端末１００および公証サーバ２００の処理を模式的に示すものである。

【００３５】

会員利用者が、会員利用者端末１００にてクライアントソフトウェアを起動すると、会員利用者端末１００は、会員利用者に対して、当該公証サービスの加入時に予めアカウント登録したユーザ名（以下、ユーザＩＤと称する）およびパスワードの入力を促す。

【００３６】

これに対して、会員利用者がユーザＩＤおよびパスワードをキーボード入力すると、会員利用者端末１００は、ログイン処理を実行し、公証サーバ２００との間にＨＴＴＰ（Hyper Text Transport Protocol）による通信リンクを確立し、公証サーバ２００に上記ユーザＩＤおよびパスワードを送信する。

【００３７】

上記ユーザＩＤおよびパスワードを受信した公証サーバ２００は、受け取ったユーザＩＤおよびパスワードの組み合わせが正しいものであるか、データベース２０１内に記録される会員登録情報を参照して検証する。

【００３８】

そして、公証サーバ２００は、受け取ったユーザＩＤおよびパスワードの組み合わせが正しいものであり、正当な会員利用者であることが確認されると、申請鍵を作成する。

【００３９】

この申請鍵は、当該申請鍵を特定するための申請鍵ＩＤと、上記会員利用者端末１００がログインを行った日時（申請時刻）と、上記会員利用者のユーザＩＤとからなり、会員利用者端末１００に送信される。

【００４０】

これに対して、会員利用者端末１００は、上記申請鍵を受信すると、公証申請の対象となる電子ファイルについての公証情報を作成する。

この公証情報には、上記電子ファイルに基づきメッセージダイジェスト技術により生成される固定長のメッセージをはじめ、上記電子ファイルについての情報（ファイル名、ファイルサイズ、最終変更日、コメント）、有効期限を示す情報が含まれる。

【００４１】

なお、以下の説明では、上記メッセージダイジェスト技術として、例えばRFC1321で規定されるＭＤ５（Message Digest Algorithm 5）を用いる場合を例に説明する。

【００４２】

ＭＤ５は、一方向ハッシュ関数を使った演算により、元のデータの長さに関係なく１２８ビットのデータ（ハッシュ値）を作成するもので、このハッシュ値が上記固定長のメッセージとなる。

【００４３】

このようにして生成された、公証申請の対象となる電子ファイルについての公証情報は、公証サーバ２００より受信した申請鍵ＩＤと組み合わされて、１つのパッケージとなり、登録情報として公証サーバ２００に送信される。

【００４４】

公証サーバ２００は、上記登録情報を受信すると、これより申請鍵ＩＤを取り出し、その正当性を検証する。

この検証の結果、取り出した申請鍵ＩＤが正当なものであることが分かると、上記登録情報内の情報に基づいて、登録鍵を作成する。

【００４５】

この登録鍵は、当該登録鍵を特定するための登録鍵ＩＤ、上記会員利用者端末

１００より登録情報を受信した日時（登録時刻）、上記申請鍵ＩＤ、上記登録情報内に含まれる電子ファイルの固定長のメッセージ（ハッシュ値）、電子ファイルについての情報（ファイル名、ファイルサイズ、最終変更日、コメント）、および有効期限を示す情報からなる。

そして、公証サーバ２００は、登録鍵内の情報のうち、登録鍵ＩＤを会員利用者端末１００に送信する。

【００４６】

これに対して、会員利用者端末１００は、上記登録鍵ＩＤを受信すると、会員利用者に対して、上記電子ファイルを公証登録してよいか、最終的な確認を行う。この確認は、パッド１０１を通じた署名入力により行われる。

会員利用者端末１００は、パッド１０１より署名入力が行われると、これに基づくサイン情報を作成し、本人特定情報として公証サーバ２００に送信する。

【００４７】

公証サーバ２００は、上記本人特定情報を受信すると、この本人特定情報が示す署名入力のサイン情報が本人の自署によるものであるかを判定する。この判定処理では、所定のアルゴリズムに従って、データベース２０１に予め記録される上記会員利用者の署名データと、上記サイン情報を比較することにより、その正当性の判定が行われる。

【００４８】

ここで、本人の自署によるものであることが判ると、公証サーバ２００は、上記申請鍵および登録鍵を公証情報としてデータベース２０１に登録し、会員利用者端末１００との間の通信リンクを切断し、当該処理を終了する。

一方、会員利用者端末１００では、公証サーバ２００より受け取った登録鍵ＩＤを保存する。

【００４９】

次に、電子ファイルと登録鍵ＩＤを入手した一般利用者が一般利用者端末３００を通じて、上記電子ファイルが公証されたものであるか公証サーバ２００に判定を求め、公証サーバ２００が上記判定を行う際の動作について説明する。図３は、この際の一般利用者端末３００および公証サーバ２００の処理を模式的に示

すものである。

【００５０】

なお、公証サーバ２００は、上記判定を求める端末からの接続要求については、一般利用者向けのクライアントソフトウェアが組み込まれている端末であれば、特に制限なく接続を許可する。

【００５１】

以下の説明では、一般利用者端末３００と公証サーバ２００との間に通信リンクを確立する処理については説明を省略し、通信リンクが確立された後の処理について説明する。

【００５２】

また、上記ソフトウェアが組み込まれていない端末が接続要求を行った場合には、上記端末に対して公証サーバ２００は、上記一般利用者向けのクライアントソフトウェアのダウンロードを促し、要求に応じて上記ソフトウェアを提供する。

【００５３】

一般利用者端末３００では、一般利用者が、当該公証サービスによって公証されたものであるか判定を求める電子ファイルと、それに対応する登録鍵ＩＤ、および公証サーバ２００との連絡に用いる電子メールアドレスを指定する。

【００５４】

すると、一般利用者端末３００は、一般利用者に指定された電子ファイルに基づいて、ＭＤ５によるハッシュ値を求め、このハッシュ値と、上記指定された登録鍵ＩＤ、電子メールアドレスを組み合わせ、公証要求情報として公証サーバ２００に送信する。

【００５５】

上記公証要求情報を受信した公証サーバ２００は、上記公証要求情報からハッシュ値と登録鍵ＩＤを取り出す。そして、この取り出した登録鍵ＩＤが、公証情報としてデータベース２０１に登録されているか否かを判定する。

【００５６】

ここで、登録が確認されると、公証サーバ２００は、上記データベース２０１

から上記登録鍵ＩＤに対応する公証情報内のハッシュ値を読み出し、上記公証要求情報から取り出したハッシュ値と一致するか検証する。

【００５７】

このようにして、登録鍵ＩＤの存在確認と、それに対応するハッシュ値の一致が確認されると、公証サーバ２００は、これらの確認がなされた旨を示す確認情報を作成し、一般利用者端末３００に送信するとともに、公証要求を受けた日時をデータベース２０１に記録する。

これに対して、一般利用者端末３００は、確認情報を受信すると、公証サーバ２００に対して当該電子ファイルの証明書の発行を要求（公証要求）する。

【００５８】

公証サーバ２００は、上記公証要求を受け付けると、データベース２０１に記録される公証情報に基づいて、当該電子ファイルの証明書を作成する。なお、この証明書には、公証対象となった電子ファイルの公証登録の日時、登録者の氏名（ユーザＩＤに対応する氏名）、ファイル名、ハッシュ値の他、書誌事項が含まれている。

そして、公証サーバ２００は、作成した証明書を一般利用者端末３００に送信し、これを一般利用者端末３００が受信し、当該処理を終了する。

【００５９】

次に、会員利用者が会員利用者端末１００を通じて、任意の電子ファイルの謄本を公証サーバ２００に登録する際の動作について説明する。図４は、この際の会員利用者端末１００および公証サーバ２００の処理を模式的に示すものである。

【００６０】

なお、以下の説明では、会員利用者端末１００と公証サーバ２００との間に通信リンクを確立する処理については、図２の説明と同様であることより、説明を省略し、通信リンクが確立された後の処理について説明する。

【００６１】

会員利用者端末１００では、会員利用者が、謄本として登録したい電子ファイルと、これに対応する登録鍵ＩＤ（図２に示した処理で取得済）を指定すると、

会員利用者端末１００は、上記電子ファイルからＭＤ５によるハッシュ値を求め、このハッシュ値と、上記電子ファイルおよび登録鍵ＩＤをパッケージ化して、公証サーバ２００に送信する。

【００６２】

パッケージを受信した公証サーバ２００は、保存内容を確認する処理として、上記パッケージから登録鍵ＩＤとハッシュ値を取り出し、この登録鍵ＩＤが、①すでに公証サーバ２００に登録されている登録鍵ＩＤと一致するか、②上記謄本登録要求した会員利用者によって登録されたものであるか、そして③取り出したハッシュ値が上記登録鍵ＩＤに対応する登録鍵内のハッシュ値と一致するか、④パッケージから取り出した電子ファイルからＭＤ５によるハッシュ値を求め、このハッシュ値と一致するか、をそれぞれ検証する。

【００６３】

この検証の結果、上記条件①～④全てを満足することが確認されると、公証サーバ２００は、保存準備処理として、上記パッケージ内の電子ファイルを仮保存するとともに、上記電子ファイルが登録鍵ＩＤに対応するものであることが確認できた旨を示す確認情報を作成し、これを会員利用者端末１００に送信する。

【００６４】

これに対して、会員利用者端末１００は、会員利用者に対して、上記電子ファイルを謄本として登録してよいか、最終的な確認を行う。この確認は、パッド１０１を通じた署名入力により行われる。

会員利用者端末１００は、パッド１０１より署名入力が行われると、これに基づいてサイン情報を作成し、本人特定情報として公証サーバ２００に送信する。

【００６５】

公証サーバ２００は、上記本人特定情報を受信すると、この本人特定情報が示すサイン情報が本人の自署によるものであるかを判定する。この判定処理では、所定のアルゴリズムに従って、上記サイン情報を、データベース２０１に予め記録される署名データと比較することにより、その正当性の判定が行われる。

【００６６】

ここで、本人の自署によるものであることが判ると、公証サーバ２００は、仮

保存していた電子ファイルを正式に謄本としてデータベース２０１に登録し、会員利用者端末１００に登録の完了を通知して通信リンクを切断し、当該処理を終了する。

【００６７】

次に、会員利用者が会員利用者端末１００を通じて公証サーバ２００に対し、謄本として登録される電子ファイルを受け取るためのデータを一般利用者端末３００に電子メールで送信させる際の動作について説明する。図５は、この際の会員利用者端末１００および公証サーバ２００の処理を模式的に示すものである。

【００６８】

なお、以下の説明では、会員利用者端末１００と公証サーバ２００との間に通信リンクを確立する処理については、図２の説明と同様であることより説明を省略し、通信リンクが確立された後の処理について説明する。

【００６９】

会員利用者端末１００は、公証サーバ２００との間に通信リンクが確立されると、保存しておいた所望の登録鍵ＩＤに、謄本取得を許可する一般利用者の電子メールアドレスと、有効期限、その他の制御情報を付加した送信情報を生成し、この送信情報を公証サーバ２００に送信する。

【００７０】

上記送信情報を取得した公証サーバ２００は、上記送信情報より登録鍵ＩＤを取り出し、この登録鍵ＩＤが、①すでに公証サーバ２００に登録されている登録鍵ＩＤと一致するか、②上記謄本登録要求した会員利用者によって登録されたものであるか、をそれぞれ検証する。

【００７１】

この検証の結果、上記条件①、②共に満足することが確認されると、公証サーバ２００は、請求鍵を作成する。

なお、この請求鍵は、当該請求鍵を特定するための請求鍵ＩＤと、会員利用者端末１００より上記送信情報を受信した日時（登録時刻）、上記送信情報に含まれる登録鍵ＩＤ、電子メールアドレス（送付先）、有効期限、その他の制御情報からなる。

【００７２】

また、上記送信情報にて複数の電子メールアドレスが指定される場合には、公証サーバ２００は、その数だけ請求鍵を生成する。

そして、公証サーバ２００は、会員利用者端末１００に対して、上記請求鍵内の情報のうち、請求鍵ＩＤを確認情報として送信する。

【００７３】

これに対して、会員利用者端末１００は、上記確認情報を受信すると、会員利用者に対して、上記電子ファイルの謄本取得を、電子メールアドレスで指定した一般利用者に許可してよいか、最終的な確認を行う。

【００７４】

この確認は、パッド１０１を通じた署名入力により行われる。

会員利用者端末１００は、パッド１０１より署名入力が行われると、これに基づいてサイン情報を作成し、本人特定情報として公証サーバ２００に送信する。

【００７５】

公証サーバ２００は、上記本人特定情報を受信すると、この本人特定情報が示すサイン情報が本人の自署によるものであるかを判定する。この判定処理では、所定のアルゴリズムに従って、上記サイン情報を、データベース２０１に記録される署名データと比較することにより、その正当性の判定が行われる。

【００７６】

ここで、本人の自署によるものであることが判ると、公証サーバ２００は、上記請求鍵を送信情報としてデータベース２０１に登録するとともに、上記請求鍵ＩＤを自己の持つＷｅｂ上に登録した後、会員利用者端末１００に登録の完了を通知して通信リンクを切断する。なお、上記ＷｅｂのＵＲＬは、会員利用者端末１００より通知された（送付先として指定された）上記電子メールアドレス毎に固有に設定されるものである。

【００７７】

そしてさらに、公証サーバ２００は、上記電子メールアドレス宛てに、この電子メールアドレスに対応する上記ＵＲＬの情報が含まれている電子メールを送信し、当該処理を終了する。

【００７８】

次に、一般利用者が一般利用者端末３００を通じて、公証サーバ２００に謄本登録される電子ファイルを取得する際の動作について説明する。図６は、この際の一般利用者端末３００および公証サーバ２００の処理を模式的に示すものである。

【００７９】

なお、公証サーバ２００に謄本登録される電子ファイルを取得するには、図２の処理で発行された登録鍵ＩＤ、あるいは図５の処理で生成された請求鍵ＩＤが必要となる。

【００８０】

その取得方法としては、一般利用者が、電子ファイルを謄本登録した利用者から直接取得することも考えられる。しかし、以下の説明では、当該システムでは最も一般的と考えられる、公証サーバ２００のＷｅｂより請求鍵ＩＤを取得する場合について説明する。

【００８１】

まず、一般利用者端末３００は、図５に示した処理により公証サーバ２００が送信する電子メールを受信すると、ブラウザソフトウェアを用いて、この電子メールに記載されるＵＲＬに対応するＷｅｂの閲覧を開始する。そして、一般利用者端末３００は、上記Ｗｅｂより請求鍵ＩＤを取得する。

【００８２】

上記Ｗｅｂは、図５でも示したように、公証サーバ２００上に設けられており、一般利用者端末３００により請求鍵ＩＤが取得されると、公証サーバ２００は、その日時をデータベース２０１に記録する。

【００８３】

一方、一般利用者端末３００では、一般利用者の要求に応じて、上記請求鍵ＩＤと自己の電子メールアドレスをパッケージ化して、謄本要求情報として公証サーバ２００に送信する。

【００８４】

上記謄本要求情報を受信した一般利用者端末３００は、上記謄本要求情報より

請求鍵ＩＤと電子メールアドレスを取り出す。そして、この取り出した請求鍵ＩＤと電子メールアドレスとが対応づけられて、送信情報としてデータベース２０１に登録されているか否かを判定する。

【００８５】

ここで、登録が確認されると、公証サーバ２００は、請求鍵ＩＤの利用者が正当なものであると判断し、データベース２０１から上記請求鍵ＩＤに対応する電子ファイルを読み出し、この電子ファイルからＭＤ５によるハッシュ値を生成する。

【００８６】

そして、公証サーバ２００は、上記電子ファイル、上記ハッシュ値、上記電子ファイルの謄本登録日時、登録者、ファイル名、当該要求日時などの情報をパッケージ化し、謄本情報として一般利用者端末３００に送信する。

【００８７】

これに対して、一般利用者端末３００は、受信した謄本情報から、電子ファイルを取り出し、この電子ファイルからＭＤ５によるハッシュ値を生成する。そして、この生成したハッシュ値と、上記謄本情報内のハッシュ値を比較することにより、正常な受信がなされたかを確認する。

【００８８】

ここで、正常な受信が確認されると、一般利用者端末３００は、これらの確認がなされた旨を示す確認情報を作成して、公証サーバ２００に送信し、公証サーバ２００との間の通信リンクを切断し、当該処理を終了する。

【００８９】

以上のように、上記構成の電子公証システムでは、公証サーバ２００にて予め認証されているネットワークユーザ（会員利用者）が、公証対象となる電子ファイルの固有情報（ハッシュ値）を作成し、公証サーバ２００は、サイン入力により上記ユーザが識別されると、上記固有情報と上記ユーザの識別情報を対応づけ、登録鍵ＩＤとともに自己のデータベース２０１に保存し、上記登録鍵ＩＤを上記ユーザにのみ報知する。

【００９０】

そして、一般利用者（もしくは会員利用者）が、手元の電子ファイルが公証されたものであるか確認する場合には、上記電子ファイルよりハッシュ値を作成し、このハッシュ値と、電子ファイルとともに入手した登録鍵ＩＤをネットワークを通じて公証サーバ２００に送信し、公証されたものであるか確認要求を行う。

【００９１】

これに対して、公証サーバ２００は、受信した登録鍵ＩＤに対応するハッシュ値をデータベース２０１より読み出し、このハッシュ値と、公証確認要求者より受信したハッシュ値が一致する場合には、その旨を示す公証情報を作成し、公証確認要求者に送信するようにしている。

【００９２】

したがって、上記構成の電子公証システムによれば、悪意を有する第三者が、会員利用者になりすまして電子ファイルを公証登録しようとしても、会員利用者のユーザＩＤやパスワード、サイン入力によるユーザ識別情報を入力する必要があるため、なりすましによる不正公証登録を確実に防止できる。

【００９３】

すなわち、公証サーバ２００により公証される電子ファイルは、公証人役場で公証される紙媒体の公正証書と同様に、真正性が保証された公証が行われたものであり、公証確認要求者はネットワークを通じて迅速かつ正確な公証サービスを受けることができる。

【００９４】

また、公証サーバ２００は、電子ファイルのハッシュ値を公証情報としてデータベース２０１に記録するにあたり、会員利用者から公証登録の要求があった日時の情報をあわせて記録するようにしているので、同じ会員利用者から同一の取引などに関して複数の登録がなされた場合でも、その要求日時より有効な電子ファイルを識別することができる。

【００９５】

さらに、上記構成の電子公証システムでは、公証サーバ２００に対して、すでに公証されている電子ファイルと、そのハッシュ値を送信して、会員利用者が謄本登録を要求すると、サイン入力による本人識別後、公証サーバ２００は、受信

した電子ファイルを謄本として登録する。

【００９６】

上記会員利用者が、公証サーバ２００に対して謄本の送付要求を行うと、公証サーバ２００は、上記謄本を取得可能な請求鍵ＩＤを載せたＷｅｂを作成し、上記送付要求にて指定される電子メールアドレス宛てに、上記ＷｅｂのＵＲＬを通知する電子メールを送信する。

【００９７】

そして、上記電子メールを取得したネットワークユーザ（一般利用者もしくは会員利用者）は、ブラウザソフトウェア用いて、上記Ｗｅｂを閲覧して、請求鍵ＩＤを取得し、これを用いて謄本を取得し、これに対して公証サーバ２００は、この取得がなされた日時を記録するようにしている。

【００９８】

したがって、上記構成の電子公証システムによれば、悪意を有する第三者が、会員利用者になりすまして電子ファイルを謄本登録しようとしても、会員利用者のユーザＩＤやパスワード、サイン入力によるユーザ識別情報を入力する必要があるため、なりすましによる不正な謄本登録を確実に防止できる。

【００９９】

すなわち、公証サーバ２００に謄本登録される電子ファイルは、公証人役場で公証される紙媒体の公正証書と同様に、真正性が保証された謄本が登録されたものであり、謄本の提供要求者はネットワークを通じて迅速かつ正確に謄本を取得することができる。

【０１００】

また、公証サーバ２００は、電子ファイルの公証、および電子ファイルの謄本を提供するにあたり、ネットワークユーザから公証要求や謄本提供の要求があった日時をデータベース２０１に記録するようにしているので、これらの要求の発生を把握することができる。また、上述のように要求のあった日時だけでなく、公証の証明を発行した日時や、謄本を提供した日時を記録するようにしてもよい。

【０１０１】

尚、この発明は上記実施の形態に限定されるものではない。例えば、上記実施の形態では、図４に示したように、電子ファイルの謄本としての登録処理は、図２に示した処理により、予め公証登録を行った後に行うものとして説明したが、これに限定されるものではない。

【０１０２】

例えば、図２に示した処理において、会員利用者端末１００が登録情報内に謄本登録したい電子ファイルを含めて送信し、そして、所定の条件を満たす場合に、公証サーバ２００が登録鍵ＩＤを発行するようにしてもよい。

【０１０３】

このように、電子ファイルの謄本登録に先立って予め公証登録しない構成であっても、悪意を有する第三者が、会員利用者になりすまして電子ファイルを謄本登録することは不可能であり、なりすましによる不正な謄本登録を確実に防止できる。

【０１０４】

また、図６に示した謄本の提供処理では、電子メールにて通知されるＵＲＬに対応するＷｅｂを参照して請求鍵ＩＤを入手し、これを用いて謄本を取得するものとして説明したが、これに限定されるものではない。

【０１０５】

例えば、何らなの方法により登録鍵ＩＤを取得したネットワークユーザからの要求に応じて、謄本を提供するようにしてもよい。なお、この場合には、要求者に対して、第三者により認証されたデジタル証明書や、電子メールアドレスの通知を要求し、これらの情報と、予めデータベース２０１に記憶しておいた許可される者の情報を参照し、一致が確認された場合にのみ謄本を提供することにより、不正な謄本取得を防止できる。また、これらの設定を、謄本の登録者が任意に設定するようにしてもよい。

【０１０６】

さらに、上記実施の形態では、会員利用者の認証を、パッド１０１を通じたサイン入力で行うものと説明したが、これに代わって例えば、虹彩認証や声紋認証、指紋認証などのバイオメトリック認証や、その他、ＩＣカードによる個人認証

を適用することも可能である。

【０１０７】

さらにまた、会員利用者端末１００および一般利用者端末３００は、通常のパーソナルコンピュータを利用可能である。そして、この実施形態で説明した各端末の処理は、それぞれ組み込まれるクライアントソフトウェアを、上記パーソナルコンピュータが搭載するマイクロプロセッサが実行し、ネットワーク通信機能を利用して実現できる。

【０１０８】

このため、ネットワーク通信可能なパーソナルコンピュータを所有する者であれば、上記クライアントソフトウェアを組み込むだけ、上記公証サービスの恩恵を受けることができる。

【０１０９】

そしてまた、上記実施の形態では、会員利用者端末および一般利用者端末の各クライアント端末は、ハードディスクに組み込んだクライアントソフトウェアに基づいて動作するものとした。

これに代わり例えば、クライアント端末から要求が生じるたびに、公証サーバが上記要求に該当するＪＡＶＡアプレットを提供し、クライアント端末は、提供された上記アプレットに基づいて、上記クライアントソフトウェアと同様の処理動作を実現するようにしてもよい。このような構成によれば、予めクライアント端末がクライアントソフトウェアを入手したり、公証サーバよりダウンロードする必要がない。

【０１１０】

また、申請鍵ＩＤ、登録鍵ＩＤおよび請求鍵ＩＤは、例えばＲＳＡ（Rivest-Shamir-Adleman Scheme）方式により暗号化処理を施して生成するものとしてもよい。

その他、この発明の要旨を逸脱しない範囲で種々の変形を施しても同様に実施可能であることはいうまでもない。

【０１１１】

【発明の効果】

以上述べたように、この発明では、電子ファイルの公証登録を行なう場合には、第１の端末装置にて、予め与えられた第２のユーザ識別情報を用いて公証サーバとの間に通信リンクを開設し、公証対象となる電子ファイルの固有のメッセージデータを作成して公証サーバに送信する。

【０１１２】

これに対して公証サーバは、第１の端末装置よりメッセージデータを受信すると、登録鍵を作成し、第１の端末装置から送られる第１のユーザ識別情報に基づいて、第１の端末装置のユーザが正当な者であることを識別すると、上記登録鍵を上記電子ファイルに対応づけて記憶する。

【０１１３】

一方、手元の電子ファイルが公証されたものであるか確認する場合には、第２の端末装置により、上記電子ファイルの固有のメッセージデータを作成し、このメッセージデータと、電子ファイルとともに入手した登録鍵を公証サーバに送信する。

【０１１４】

これに対して、公証サーバは、受信した登録鍵に対応するメッセージデータを読み出し、このメッセージデータと、第２の端末装置より受信したメッセージデータが一致する場合には、その旨を示す公証情報を作成し、第２の端末装置に送信するようにしている。

【０１１５】

したがって、この発明によれば、悪意を有する第三者が、第１の端末装置のユーザになりすまして電子ファイルを公証登録しようとしても、上記ユーザの識別情報や、バイオメトリック情報などの第１のユーザ識別情報の入力が必要なため、なりすましによる不正公証登録を確実に防止できる。

【０１１６】

すなわち、公証サーバにより公証される電子ファイルは、公証人役場で公証される紙媒体の公正証書と同様に、真正性が保証された公証が行われたものであり、公証確認を求める者はネットワークを通じて迅速かつ正確な公証サービスを受けることが可能な電子公証システムおよび電子公証方法を提供できる。

【０１１７】

また、この発明では、電子ファイルの謄本登録を行なう場合には、第１の端末装置にて、予め与えられた第２のユーザ識別情報を用いて公証サーバとの間に通信リンクを開設し、謄本となる電子ファイルを公証サーバに送信する。

【０１１８】

これに対して公証サーバは、第１の端末装置より電子ファイルを受信すると、請求鍵を作成し、第１の端末装置から送られる第１のユーザ識別情報に基づいて、第１の端末装置のユーザが正当な者であることを識別すると、上記請求鍵を上記電子ファイルに対応づけて記憶する。

【０１１９】

一方、謄本登録された電子ファイルを取得する場合には、第２の端末装置より請求鍵を公証サーバに送信する。

これに対して、公証サーバは、受信した請求鍵に対応する電子ファイルを読み出し、第２の端末装置に送信するようにしている。

【０１２０】

したがって、この発明によれば、悪意を有する第三者が、第１の端末装置のユーザになりすまして電子ファイルを謄本登録しようとしても、第２のユーザ識別情報や、バイオメトリック情報をはじめとする第１のユーザ識別情報情報の入力が必要なため、なりすましによる不正謄本登録を確実に防止できる。

【０１２１】

すなわち、公証サーバに謄本登録された電子ファイルは、公証人役場で謄本登録される紙媒体の公正証書と同様に、真正性が保証された公証が行われたものであり、謄本の写しを求める者はネットワークを通じて迅速かつ正確な公証サービスを受けることが可能な電子公証システムおよび電子公証方法を提供できる。

【図面の簡単な説明】

【図１】

この発明に係わる電子公証システムの一実施形態の構成を示す図。

【図２】

図１に示した電子公証システムにおける、電子ファイルの公証情報の登録処理

を説明するための図。

【図３】

図１に示した電子公証システムにおける、電子ファイルの公証確認処理を説明するための図。

【図４】

図１に示した電子公証システムにおける、電子ファイルの謄本登録処理を説明するための図。

【図５】

図１に示した電子公証システムにおける、電子ファイルの謄本送信要求処理を説明するための図。

【図６】

図１に示した電子公証システムにおける、電子ファイルの謄本提供処理を説明するための図。

【図７】

電子署名技術を説明するための図。

【符号の説明】

１００…会員利用者端末

１０１…パッド

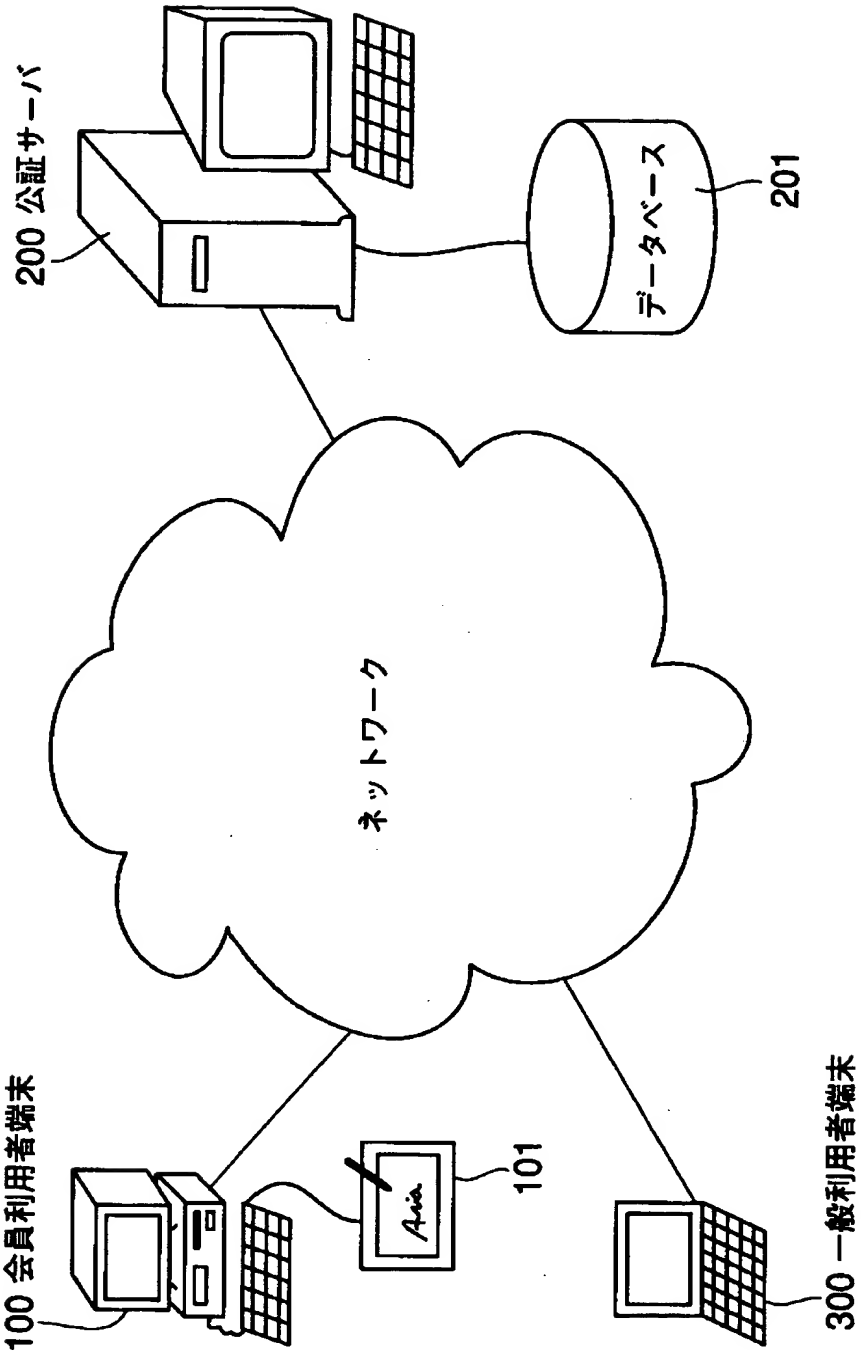
２００…公証サーバ

２０１…データベース

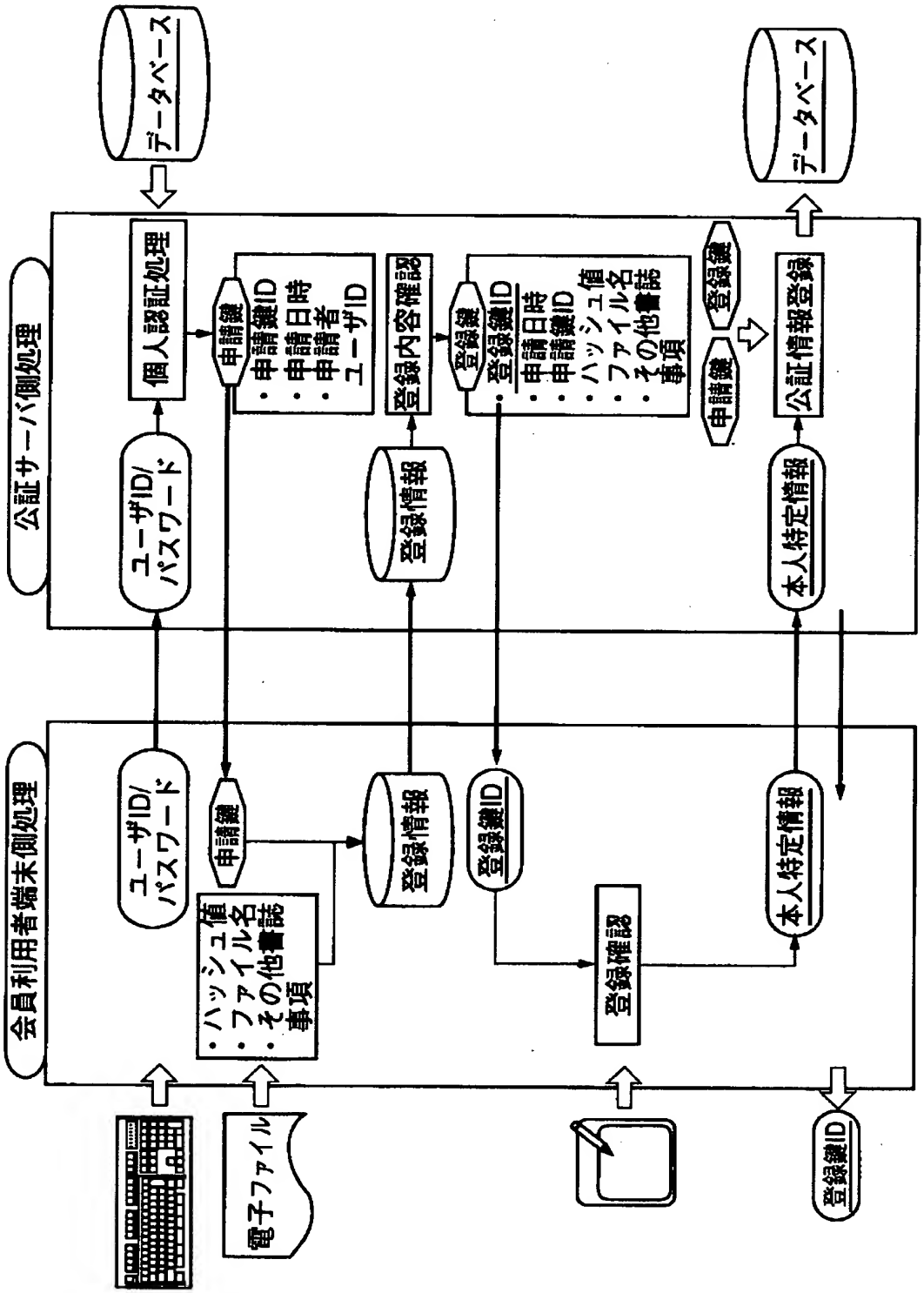
３００…一般利用者端末

【書類名】　　図面

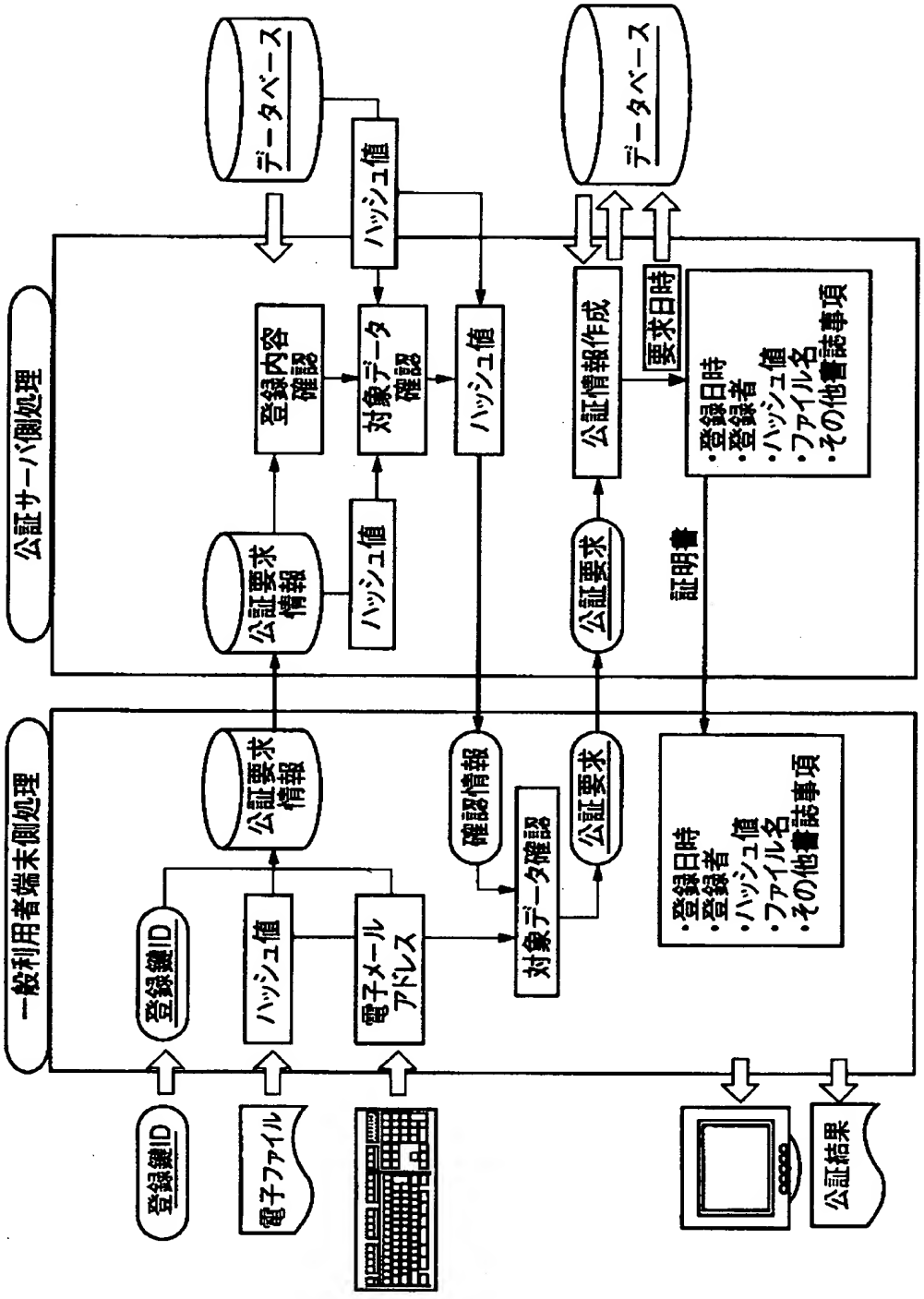
【図１】



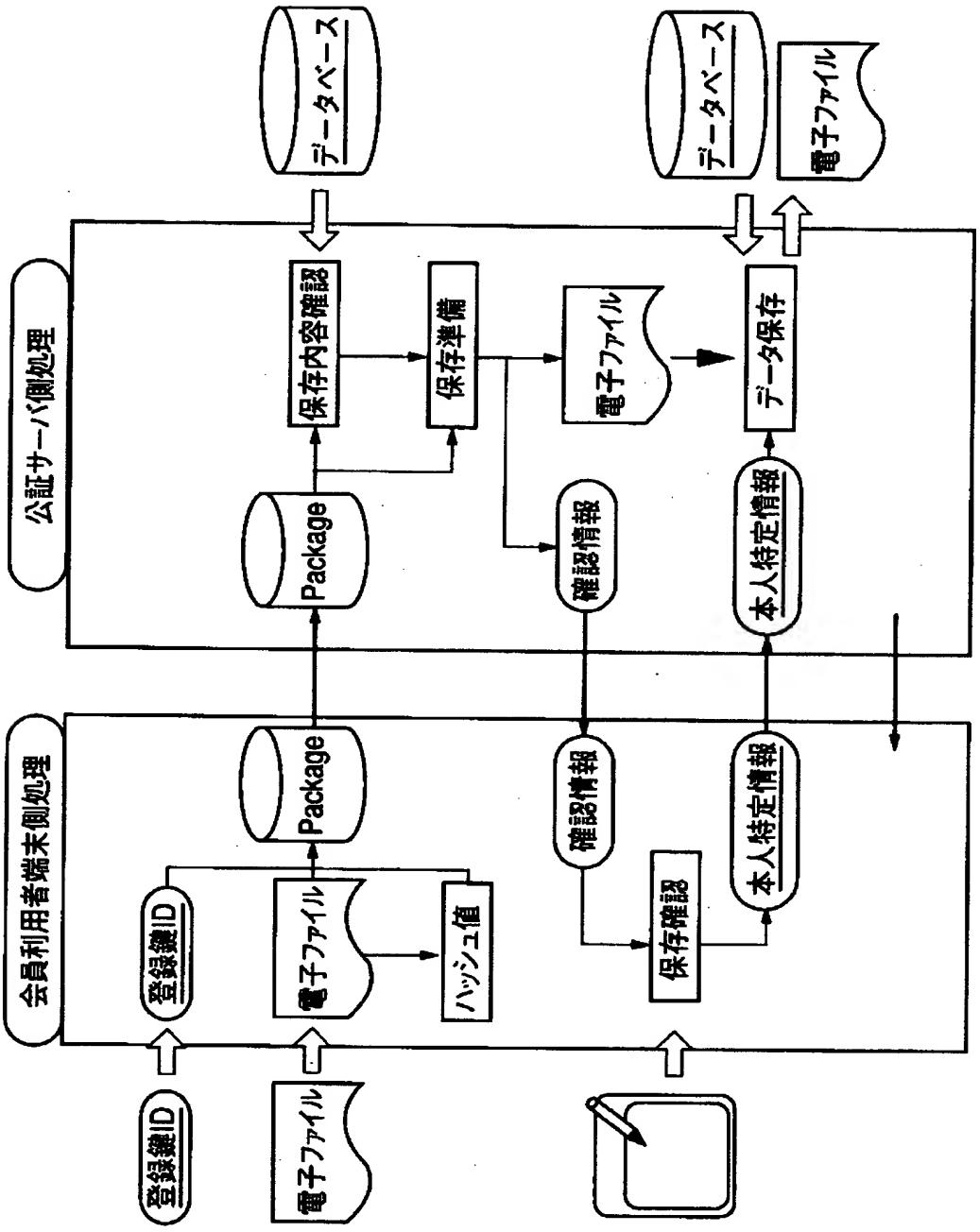
【図２】


データベース
データベース
公証サーバ側処理
個人認証処理
ユーザID/
パスワード
申請鍵
・申請鍵ID
・申請日時
・申請者
ユーザID
登録内容確認
登録情報
登録鍵
・登録鍵ID
・申請鍵ID
・申請日時
・ハッシュ値
・ファイル名
・その他
事項
申請鍵
登録鍵
公証情報登録
本人特定情報
会員利用者端末側処理
ユーザID/
パスワード
申請鍵
・ハッシュ値
・ファイル名
・その他
事項
登録情報
登録鍵ID
登録確認
本人特定情報
電子ファイル
登録鍵ID

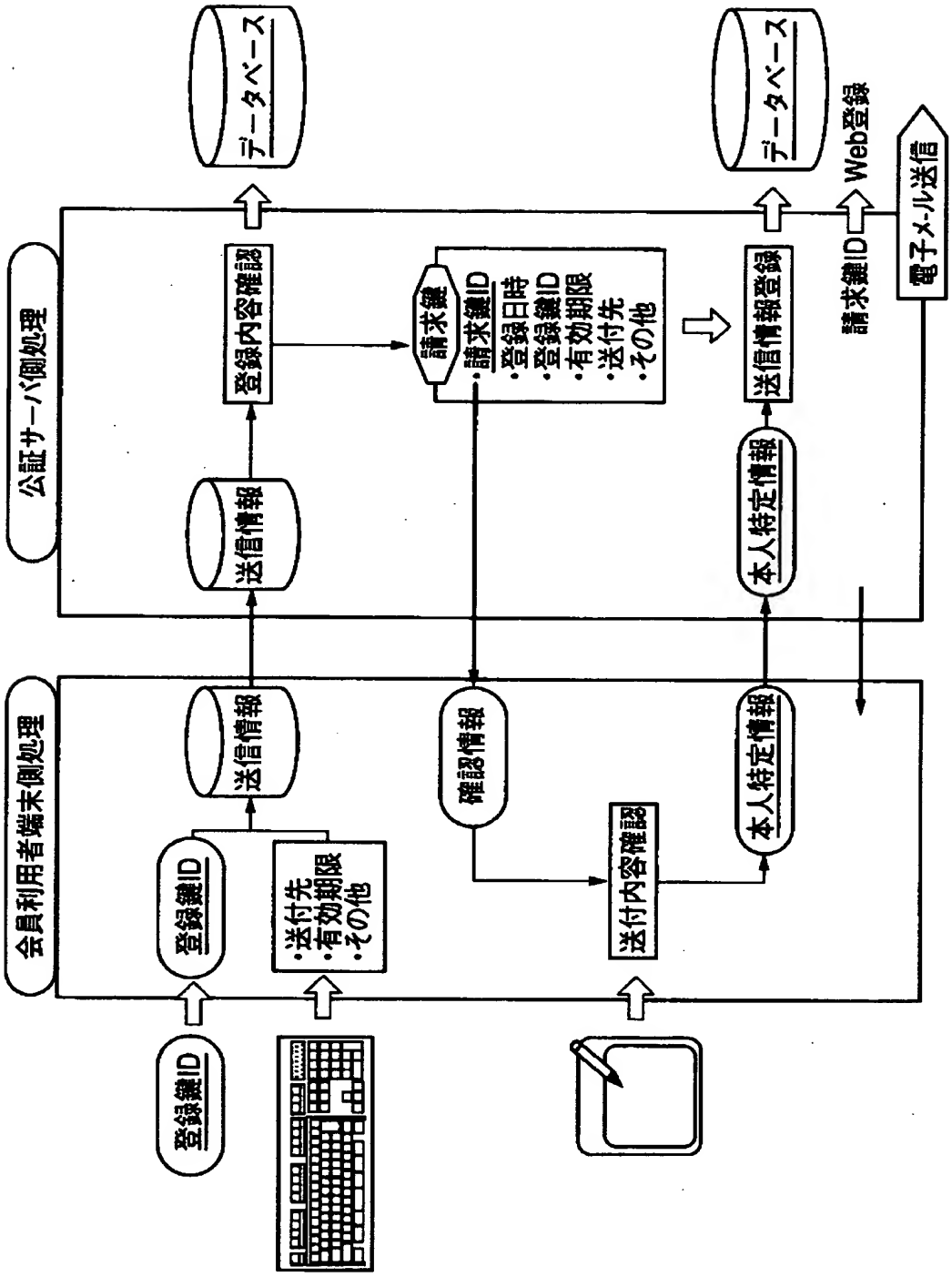
【図３】


データベース
ハッシュ値
登録内容確認
対象データ確認
ハッシュ値
公証要求情報
ハッシュ値
公証サーバ側処理
データベース
公証情報作成
要求日時
・登録日時
・登録者
・ハッシュ値
・ファイル名
・その他書誌事項
公証要求
証明書
公証要求情報
確認情報
公証要求
対象データ確認
登録鍵ID
ハッシュ値
電子メールアドレス
一般利用者端末側処理
・登録日時
・登録者
・ハッシュ値
・ファイル名
・その他書誌事項
登録鍵ID
電子ファイル
公証結果

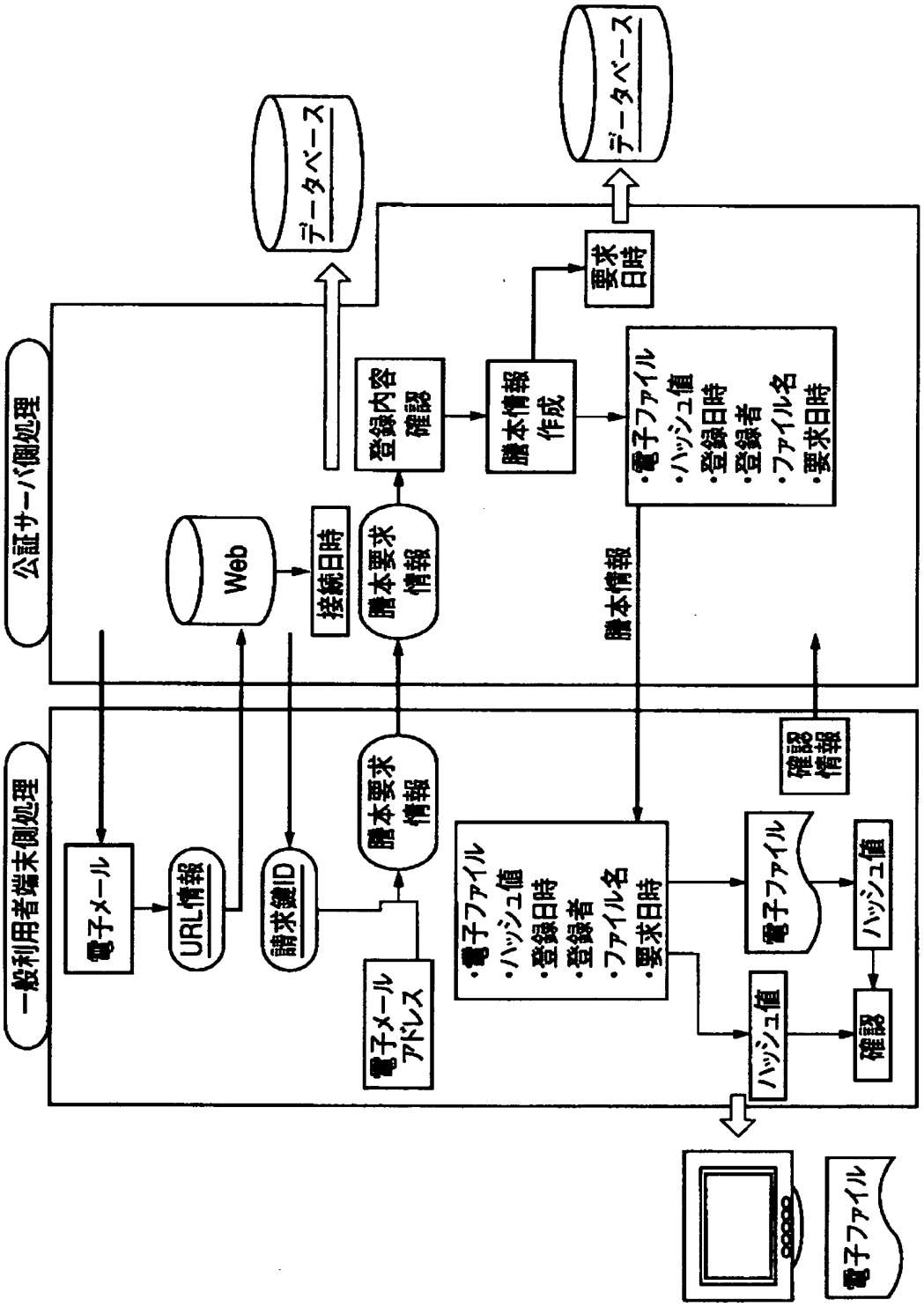
【図４】


データベース
データベース
電子ファイル
公証サーバ側処理
保存内容確認
保存準備
電子ファイル
データ保存
Package
確認情報
本人特定情報
会員利用者端末側処理
Package
確認情報
本人特定情報
登録鍵ID
電子ファイル
ハッシュ値
保存確認
登録鍵ID
電子ファイル

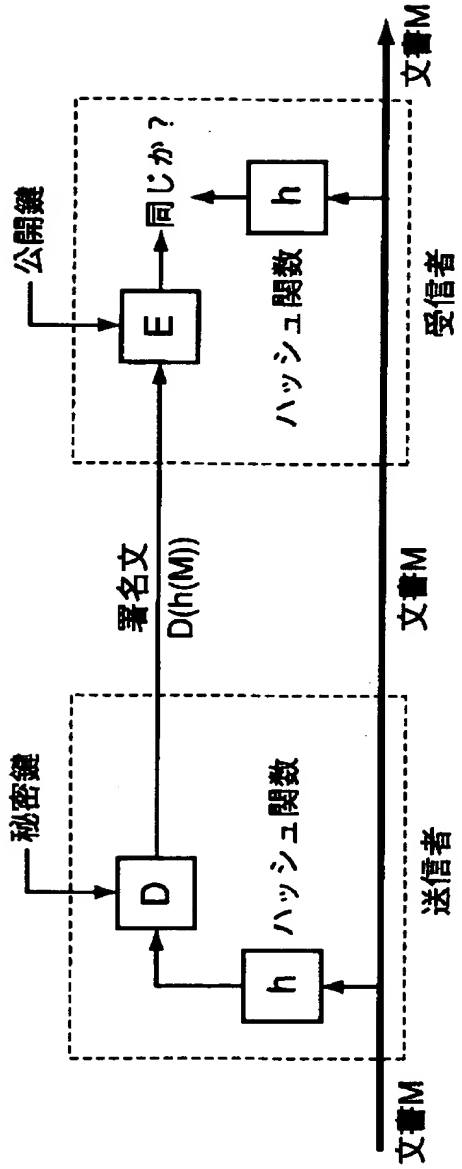
【図５】


データベース
データベース
Web登録
電子メール送信
請求鍵ID
公証サーバ側処理
登録内容確認
請求鍵
・請求鍵ID
・登録日時
・登録鍵ID
・有効期限
・送付先
・その他
送信情報登録
送信情報
本人特定情報
会員利用者端末側処理
送信情報
確認情報
本人特定情報
登録鍵ID
・送付先
・有効期限
・その他
送付内容確認
登録鍵ID

【図６】


データベース
データベース
公証サーバ側処理
一般利用者端末側処理
要求日時
登録内容確認
謄本情報作成
・電子ファイル
・ハッシュ値
・登録日時
・登録者
・ファイル名
・要求日時
Web
接続日時
謄本要求情報
謄本情報
電子メール
URL情報
請求鍵ID
謄本要求情報
電子メールアドレス
・電子ファイル
・ハッシュ値
・登録日時
・登録者
・ファイル名
・要求日時
確認情報
電子ファイル
ハッシュ値
ハッシュ値
確認
電子ファイル

【図７】



【書類名】　　要約書

【要約】

【課題】　ネットワーク上でやりとりされる文書に対して、信頼性の高い公証を行うことが可能な電子公証システムおよび電子公証方法を提供する。

【解決手段】　会員利用者は会員利用者端末１００にて、公証対象となる電子ファイルの固有情報を作成し、公証サーバ２００は、サイン入力により上記会員利用者を識別すると、上記固有情報と会員利用者の識別情報を対応づけ、登録鍵ＩＤとともにデータベース２０１に保存し、登録鍵ＩＤを会員利用者に送信する。一般利用者が、上記電子ファイルの公証確認を行う場合には、一般利用者端末３００を用いて、上記電子ファイルより固有情報を作成し、上記電子ファイルとともに入手した登録鍵ＩＤとともに公証サーバ２００に送信する。これに対して、公証サーバ２００は、受信した固有情報と、データベース２０１の固有情報が一致する場合に、公証情報を一般利用者に送信するようにしたものである。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－２０８９１３
受付番号	５００００８６８０７４
書類名	特許願
担当官	高田　良彦　　２３１９
作成日	平成１２年　７月１７日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 597095599
- 【住所又は居所】 東京都港区虎ノ門１－２５－７
- 【氏名又は名称】 亜細亜証券印刷株式会社

【特許出願人】
- 【識別番号】 500324783
- 【住所又は居所】 東京都渋谷区富ケ谷一丁目３０番２２号
- 【氏名又は名称】 株式会社シナジー・インキュベート

【代理人】 申請人
- 【識別番号】 100058479
- 【住所又は居所】 東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
- 【氏名又は名称】 鈴江　武彦

【選任した代理人】
- 【識別番号】 100084618
- 【住所又は居所】 東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
- 【氏名又は名称】 村松　貞男

【選任した代理人】
- 【識別番号】 100068814
- 【住所又は居所】 東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
- 【氏名又は名称】 坪井　淳

【選任した代理人】
- 【識別番号】 100092196
- 【住所又は居所】 東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
- 【氏名又は名称】 橋本　良郎

次頁有

認定・付加情報（続き）

【選任した代理人】
【識別番号】　100091351
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　河野　哲
【選任した代理人】
【識別番号】　100088683
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　中村　誠

次頁無

出　願　人　履　歴　情　報

識別番号　　〔５９７０９５５９９〕

１．変更年月日　　１９９７年　６月２３日
［変更理由］　新規登録
住　所　東京都港区虎ノ門１－２５－７
氏　名　亜細亜証券印刷株式会社

出　願　人　履　歴　情　報

識別番号　　〔５００３２４７８３〕

１．変更年月日　　２０００年　７月１０日
［変更理由］　新規登録
住　所　東京都渋谷区富ケ谷一丁目３０番２２号
氏　名　株式会社シナジー・インキュベート